

BRITISH STANDARD

Information security management systems –

Part 3: Guidelines for information security risk management

ICS 35.020; 35.040



NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 17 MARCH 2006

ISBN 0 580 47247 7

The following BSI references relate to the work on this standard:

Committee reference BDD/2

Draft for comment 05/30125021 DC

Publication history

First published March 2006

Amendments issued since publication

Amd. no.	Date	Text affected
-----------------	-------------	----------------------

Contents

Foreword *ii*

Introduction *1*

- 1** Scope *4*
- 2** Normative references *4*
- 3** Terms and definitions *4*
- 4** Information security risks in the organizational context *7*
- 5** Risk assessment *9*
- 6** Risk treatment and management decision-making *16*
- 7** Ongoing risk management activities *21*

Annexes

Annex A (informative) Examples of legal and regulatory compliance *26*

Annex B (informative) Information security risks and organizational risks *30*

Annex C (informative) Examples of assets, threats, vulnerabilities and risk assessment methods *33*

Annex D (informative) Risk management tools *47*

Annex E (informative) Relationship between
BS ISO/IEC 27001:2005 and BS 7799-3:2006 *48*

Bibliography *49*

List of figures

Figure 1 – Risk management process model *1*

Figure C.1 – Types of assets *33*

List of tables

Table C.1 – Vulnerabilities related to human resources security *41*

Table C.2 – Vulnerabilities related to physical and environmental security *42*

Table C.3 – Vulnerabilities related to communications and operations management *42*

Table C.4 – Vulnerabilities related to access control *43*

Table C.5 – Vulnerabilities related to systems acquisition, development and maintenance *43*

Table C.6 – Matrix with risk values *45*

Table C.7 – Matrix ranking incidents by measures of risk *46*

Table E.1 – Relationship between BS ISO/IEC 27001:2005
and BS 7799-3:2006 *48*

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 50, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 17 March 2006. It was prepared by Technical Committee BDD/2, *Information security management*.

Relationship with other publications

This British Standard includes and replaces the existing BS 7799 guidance material provided in the BSI publications PD 3002 and PD 3005.

It is harmonized with other ISO/IEC work, in particular BS ISO/IEC 17799:2005 and BS ISO/IEC 27001:2005 (the revised version of BS 7799-2:2002) to ensure consistency of terminology and methods.

Information about this document

This British Standard provides guidance and support for the implementation of BS 7799-2 and is generic enough to be of use to small, medium and large organizations. The guidance and advice given in this British Standard is not exhaustive and an organization might need to augment it with further guidance before it can be used as the basis for a risk management framework for BS ISO/IEC 27001:2005 (the revised version of BS 7799-2:2002).

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it was a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

0 Introduction

0.1 General

This British Standard has been prepared for those business managers and their staff involved in ISMS (Information Security Management System) risk management activities. It provides guidance and advice to specifically support the implementation of those requirements defined in BS ISO/IEC 27001:2005 that relate to risk management processes and associated activities. Table E.1 illustrates the relationship between the two documents.

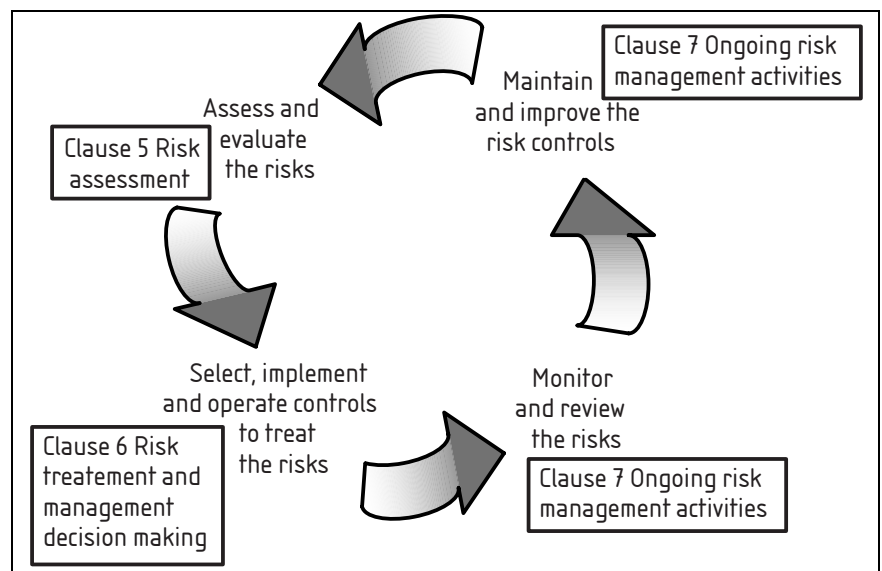
0.2 Process approach

This British Standard promotes the adoption of a process approach for assessing risks, treating risks, and ongoing risk monitoring, risk reviews and re-assessments. A process approach encourages its users to emphasize the importance of:

- understanding business information security requirements and the need to establish policy and objectives for information security;
- selecting, implementing and operating controls in the context of managing an organization's overall business risks;
- monitoring and reviewing the performance and effectiveness of the Information Security Management System (ISMS) to manage the business risks;
- continual improvement based on objective risk measurement.

See Figure 1.

Figure 1 **Risk management process model**



This risk management process focuses on providing the business with an understanding of risks to allow effective decision-making to control risks. The risk management process is an ongoing activity that aims to continuously improve its efficiency and effectiveness.

The risk management process should be applied to the whole ISMS (as specified in BS ISO/IEC 27001:2005), and new information systems should be integrated into the ISMS in the planning and design stage to ensure that any information security risks are appropriately managed. This document describes the elements and important aspects of this risk management process.

The information security risks need to be considered in their business context, and the interrelationships with other business functions, such as human resources, research and development, production and operations, administration, IT, finance, and customers need to be identified, to achieve a holistic and complete picture of these risks. This consideration includes taking account of the organizational risks, and applying the concepts and ideas of corporate governance. This, together with the organization's business, effectiveness, and the legal and regulatory environment all serve as drivers and motivators for a successful risk management process. These ideas are described in more detail in Clause 4.

An important part of the risk management process is the assessment of information security risks, which is necessary to understand the business information security requirements, and the risks to the organization's business assets. As also described in BS ISO/IEC 27001:2005, the risk assessment includes the following actions and activities, which are described in more detail in Clause 5.

- Identification of assets.
- Identification of legal and business requirements that are relevant for the identified assets.
- Valuation of the identified assets, taking account of the identified legal and business requirements and the impacts of a loss of confidentiality, integrity and availability.
- Identification of significant threats and vulnerabilities for the identified assets.
- Assessment of the likelihood of the threats and vulnerabilities to occur.
- Calculation of risk.
- Evaluation of the risks against a predefined risk scale.

The next step in the risk management process is to identify the appropriate risk treatment action for each of the risks that have been identified in the risk assessment. Risks can be managed through a combination of prevention and detection controls, avoidance tactics, insurance and/or simple acceptance. Once a risk has been assessed a business decision needs to be made on what, if any, action to take. In all cases, the decision should be based on a business case which justifies the decision and which can be accepted or challenged by key stakeholders. The different risk treatment options and factors that influence this decision are described in Clause 6.

Once the risk treatment decisions have been made and the controls selected following these decisions have been implemented, the ongoing risk management activities should start. These activities include the process of monitoring the risks and the performance of the ISMS to ensure that the implemented controls work as intended. Another activity is the risk review and re-assessment, which is necessary to adapt the risk assessment to the changes that might occur over time in the business environment. Risk reporting and communication is necessary to ensure that business decisions are taken in the context of an organization-wide understanding of risks. The co-ordination of the different risk related processes should ensure that the organization can operate in an efficient and effective way. Continual improvement is an essential part of the ongoing risk management activities to increase the effectiveness of the implemented controls towards achieving the goals that have been set for the ISMS. The ongoing risk management activities are described in Clause 7.

The successful implementation of the risk management process requires that roles and responsibilities are clearly defined and discharged within the organization. Roles and responsibilities that are involved in the risk management process are included in the document, as relevant.

1 Scope

This British Standard gives guidance to support the requirements given in BS ISO/IEC 27001:2005 regarding all aspects of an ISMS risk management cycle. This cycle includes assessing and evaluating the risks, implementing controls to treat the risks, monitoring and reviewing the risks, and maintaining and improving the system of risk controls.

The focus of this standard is effective information security through an ongoing programme of risk management activities. This focus is targeted at information security in the context of an organization's business risks.

The guidance set out in this British Standard is intended to be applicable to all organizations, regardless of their type, size and nature of business. It is intended for those business managers and their staff involved in ISMS (Information Security Management System) risk management activities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO/IEC 27001:2005 (BS 7799-2:2005), *Information technology – Security techniques – Information security management systems – Requirements*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 information security event

an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [BS ISO/IEC TR 18044:2004]

3.2 information security incident

an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [BS ISO/IEC TR 18044:2004]

3.3 residual risk

risk remaining after risk treatment [ISO Guide 73:2002]

3.4 risk

combination of the probability of an event and its consequence [ISO Guide 73:2002]

3.5 risk acceptance

NOTE 1 The verb “to accept” is chosen to convey the idea that acceptance has its basic dictionary meaning.

NOTE 2 Risk acceptance depends on risk criteria.

decision to accept a risk [ISO Guide 73:2002]

3.6 risk analysis

NOTE 1 Risk analysis provides a basis for risk evaluation, risk treatment, and risk acceptance.

NOTE 2 Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.

systematic use of information to identify sources and to estimate the risk [ISO Guide 73:2002]

3.7 risk assessment

overall process of risk analysis and risk evaluation [ISO Guide 73:2002]

3.8 risk avoidance

NOTE The decision may be taken based on the result of risk evaluation.

decision not to become involved in, or action to withdraw from, a risk situation [ISO Guide 73:2002]

3.9 risk communication

NOTE The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

exchange or sharing of information about risk between the decision-maker and other stakeholders [ISO Guide 73:2002]

3.10 risk control

NOTE Risk control may involve monitoring, re-evaluation, and compliance with decisions.

actions implementing risk management decisions [ISO Guide 73:2002]

3.11 risk criteria

NOTE Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

terms of reference by which the significance of risk is assessed [ISO Guide 73:2002]

3.12 risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of risk [ISO Guide 73:2002]

3.13 risk management

NOTE Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication.

co-ordinated activities to direct and control an organization with regard to risk [ISO Guide 73:2002]

3.14 risk management system

NOTE 1 Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

NOTE 2 The culture of an organization is reflected in its risk management system.

set of elements of an organization's management system concerned with managing risk [ISO Guide 73:2002]

3.15 risk reduction

actions taken to lessen the probability, negative consequences, or both, associated with a risk [ISO Guide 73:2002]

3.16 risk transfer

NOTE 1 Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk.

NOTE 2 Risk transfer can be carried out through insurance or other agreements.

NOTE 3 Risk transfer can create new risks or modify existing risk.

NOTE 4 Relocation of the source is not risk transfer.

sharing with another party the burden of loss or benefit of gain, for a risk [ISO Guide 73:2002]

3.17 risk treatment

NOTE 1 The term risk treatment is sometimes used for the measures themselves.

NOTE 2 Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

NOTE 3 In this British Standard the term "control" is used as a synonym for "measure".

treatment process of selection and implementation of measures to modify risk [ISO Guide 73:2002]

3.18 threat

a potential cause of an incident, that may result in harm to system or organization [BS ISO/IEC 13335-1:2004]

3.19 vulnerability

a weakness of an asset or group of assets than can exploited by one or more threats [BS ISO/IEC 13335-1:2004]

4 Information security risks in the organizational context

4.1 Information security management system scope and policy

4.1.1 Business case

As the implementation of an ISMS requires the deployment of significant resources, all organizations need to be clear about their reasons for implementing such a system. Different organizations will have different business drivers for undertaking the implementation of an ISMS. These drivers will derive from their regulatory or legal position, their status as a large or small business, a publicly-funded or government organization, their geographical location, the type of business they are in, or the service they offer. The business case for implementing an ISMS should be clearly documented, and should set out the likely costs balanced against the benefits that can be derived from an increase in the ability to manage information risk.

The ISMS should not be established in isolation, but should take account of the organizational risks and the overall business strategies in the organization. Annex B explains the relationships between the different types of risk.

4.1.2 ISMS scope

Defining the ISMS scope is one of the most important decisions in the whole process, as the definition of the scope sets the scene for what will be involved in the ISMS. The definition of the scope of the ISMS is entirely up to the organization. The scope of an ISMS can be the whole organization, or suitable part(s) of the organization, or only a specific business process or information system. The scope of the ISMS should be defined in terms of the characteristics of the business, its location, assets and technology (see BS ISO/IEC 27001:2005, **4.2.1 a**)), and it should be well defined and complete, addressing the different elements mentioned in BS ISO/IEC 27001:2005.

The decision on the ISMS scope needs to take account of the interfaces and dependencies this ISMS has with other parts of the organization (not within the ISMS scope), other organizations, third party suppliers, or with any other entity outside the ISMS. An example is an ISMS that consists only of a particular business process. In this case, the other parts of the organization that the ISMS needs for its day-to-day functioning (e.g. human resources, finance, sales and marketing or facilities management) are interfaces and dependencies, in addition to all the other interfaces and dependencies that might exist.

The scope of the ISMS should be suitable and appropriate to both the organization's capability and its responsibility to provide information security that meets the requirements determined by its risk assessment and by appropriate legal and regulatory controls. Indeed, such a scope is an absolute necessity for organizations seeking to claim conformity with BS ISO/IEC 27001:2005 (see **1.2** of BS ISO/IEC 27001:2005). Also to claim this conformity nothing should be excluded from the ISMS scope which affects the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by the risk assessment and appropriate regulatory requirements.

4.1.3 ISMS policy

Having determined the scope of its ISMS, an organization should set out a clear and succinct information security policy to support the implementation of information security. BS ISO/IEC 17799:2005 states that the objective of the policy is: "To provide management direction and support for information security." The policy should be approved by management, and it should be ensured that all employees have received the policy and understand its effect on their work. This policy should include a framework for setting objectives, giving management direction and action, and establishing the risk management context and criteria against which risks will be evaluated. Management direction and support is essential because the effective management of information security risk requires the deployment of significant resources.

4.2 Risk approach/philosophy

BS ISO/IEC 27001:2005, **4.2.1 c)** requires the organization to identify and adopt a systematic method and approach to risk assessment. It is important that information security risk is managed clearly and consistently throughout an organization. However, managing the risks can employ different risk assessment and management approaches and various degrees of granularity that suit the organization's needs. It is entirely the decision of the organization which risk assessment approach is chosen. Whatever the organization decides on, it is important that the approach to risk management is suitable and appropriate to address all of the organization's requirements.

BS ISO/IEC 27001:2005, **4.2.1 c)–e)** sets the framework for the risk assessment approach to be chosen by describing the mandatory elements that the risk assessment process should contain. These mandatory elements are as follows.

- *Determination of the criteria for risk acceptance.* This should describe the circumstances under which the organization is willing to accept the risks.
- *Identification of acceptable levels of risk.* Whatever risk assessment approach is chosen, the levels of risk that the organization considers acceptable need to be identified.
- *Identification and assessment of the risks.* A number of mandatory elements need to be identified and processes carried out, described in more detail in Clause **5** of this document. It is necessary that the risk assessment approach chosen addresses all of the concepts that are discussed in Clause **5**, as listed in **5.1**.

- *Coverage of all aspects of the ISMS scope.* The risk assessment approach chosen needs to cover all control areas in BS ISO/IEC 27001:2005, Annex A. The need for such comprehensive coverage is important, as several risk assessment approaches are in use that concentrate on IT only, and are not suitable for the type of assessment required by BS ISO/IEC 27001:2005.

The risk assessment should achieve a clear understanding of what factors should be controlled, as these factors affect systems and processes that are critical to the organization. Risk management activities should nonetheless be cost-effective and pragmatic. Effective risk management means balancing the expenditure of resources against the required degree of protection and ensuring that the resources expended are correlated with the potential loss and value of the assets protected (5.4 deals with the valuation of critical information assets).

The chosen approach's level of detail and complexity influence the effort and resources required during the risk assessment process. The risk assessment should be as detailed and complex as necessary to address all of the organization's requirements and what is required for the ISMS scope, but no more. Too much detail might lead to excess work, and a too-high-level view might lead to overlooking important risk aspects. BS ISO/IEC 27001:2005 does not require a highly-technical or detailed approach, as long as all risks are appropriately addressed.

5 Risk assessment

5.1 Risk assessment process

The assessment of information security risks includes risk analysis and risk evaluation, and depends upon the following factors used in these processes. The risk analysis should include:

- identification of assets (see BS ISO/IEC 27001:2005, 4.2.1 d) and 5.2 of this standard);
- identification of legal and business requirements that are relevant for the identified assets (see 5.3);
- valuation of the identified assets, taking account of the identified legal and business requirements and the impacts resulting from a loss of confidentiality, integrity and availability (see 5.4);
- identification of significant threats and vulnerabilities for the identified assets (see BS ISO/IEC 27001:2005, 4.2.1 d) and 5.5 of the current standard); and
- assessment of the likelihood of the threats and vulnerabilities to occur (see BS ISO/IEC 27001:2005, Clause 4.2.1 e) and 5.6 of the current standard).

Risk evaluation should include:

- calculation of risk (see BS ISO/IEC 27001:2005, 4.2.1 e)3) and 5.7); and
- evaluation of the risks against a predefined risk scale (see 5.8).

5.2 Asset identification

An asset is something that has value or utility for the organization, its business operations and their continuity. Therefore, assets need protection to ensure correct business operations and business continuity. The proper management and accountability of assets¹⁾ is vital, and should be a major responsibility of all management levels.

The important assets within the scope of the ISMS should be clearly identified and appropriately valued (see BS ISO/IEC 27001:2005, **4.2.1** and **5.3** of the current standard), and an inventory of these assets should be put together and maintained. In order to make sure that no asset is overlooked or forgotten, the scope of the ISMS considered should be defined in terms of the characteristics of the business, the organization, its location, assets and technology. Examples of assets and more information about asset identification can be found in **C.1**. Grouping similar or related assets into manageable collections can help to reduce the effort necessary for the risk assessment process.

Accountability for assets helps ensure that adequate information security is maintained. An owner²⁾ should be identified for each of the identified assets, or groups of assets, and the responsibility for the maintenance of appropriate security controls should be assigned to the owner. Responsibility for implementing security controls may be delegated, although accountability should remain with the nominated owner of the asset.

The asset owner should be responsible for defining the appropriate security classification and access rights for the asset, to agree and document these decisions and to maintain appropriate security controls. It is also the owner's responsibility to periodically review the access rights and the security classifications. In addition, it might be useful to define, document and implement rules for the acceptable use of assets, describing permitted and forbidden actions in the day-to-day use of the asset. The persons using the assets should be aware of these rules as the correct use of the assets is part of their responsibilities.

5.3 Identification of legal and business requirements

5.3.1 Sources of requirement

Security requirements in any organization, large or small, are in effect derived from three main sources and should be documented in the ISMS.

- The unique set of threats and vulnerabilities which could lead to significant losses if they occur (these are considered in **5.5**).
- The legal, statutory and contractual requirements which are applicable to the organization, its trading partners, contractors and service providers.

¹⁾ Clause **7** of BS ISO/IEC 17799:2005 defines two specific objectives with regard to assets: accountability for assets (in **7.1**) and information classification (in **7.2**).

²⁾ The term "owner" identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.

- The unique set of principles, objectives and requirements for information processing that an organization has developed to support its business operations and processes, and which apply to the organization's information systems.

Once these legal and business requirements have been identified, it is necessary to consider them in the asset valuation process (see **5.4**) and formulate them in terms of requirements for confidentiality, integrity, and availability.

5.3.2 Legal, regulatory and contractual requirements

The security requirements relating to the set of statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and services providers have to satisfy, should be documented in an ISMS. It is important, e.g. for the control of proprietary software copying, safeguarding of organizational records, or data protection, that the ISMS supports these requirements, and it is vital that the implementation, or absence, of security controls in each of the information systems does not breach any statutory, legal or civil obligations, or commercial contracts. Therefore, the legal statutory and contractual requirements related to each of the assets and to the organization should be identified. More information about legal and regulatory compliance is provided in Annex A.

5.3.3 Organizational principles, objectives and business requirements

The security requirements relating to the organization-wide principles, objectives and requirements for information processing to support its business operations should also be documented in an ISMS. It is important, e.g. for competitive edge, cash flow and/or profitability, that the ISMS supports these requirements, and vital that the implementation, or absence, of security controls in each of the information systems does not impede efficient business operations. For each of the assets and the business activities within the organization, the related business objectives and requirements should be identified.

5.4 Asset valuation

Asset identification and valuation, based on the business needs of an organization, are major factors in risk assessment. In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business or their potential values in different business opportunities. It is also important to take account of the identified legal and business requirements (see **5.3**) and the impacts resulting from a loss of confidentiality, integrity and availability.

One way to express asset values is to use the business impacts that unwanted incidents, such as disclosure, modification, non-availability and/or destruction, would have to the asset and the related business interests that would be directly or indirectly damaged. These incidents could, in turn, lead to loss of revenue or profit, market share, or image and reputation, and these considerations should be reflected in the asset values.

The input for the valuation of assets should be provided by owners and users of assets, who can speak authoritatively about the importance of assets, particularly information, to the organization and its business, and how the assets are used to support the business processes and objectives. In order to consistently assess the asset values, a valuation scale for assets should be defined. More information about asset valuation scales can be found in **C.5.1**.

For each of the assets, values should be identified that express the potential business impacts if the confidentiality, integrity or availability, or any other important property of the asset is damaged. An individual value should be identified for each of these properties as these are independent and can vary for each of the assets.

Information and other assets, as appropriate, should be classified in accordance with the identified asset value, legal or business requirements and criticality (see BS ISO/IEC 17799:2005, Clause **7.2**). Classification indicates the need, priorities and expected degree of protection when handling the information. It should be the responsibility of the asset owner (see also **5.2**) to define the classification, as well as reviewing it to ensure that the classification remains at the appropriate level.

5.5 Identification and assessment of threats and vulnerabilities

5.5.1 Implemented controls

At some point, either prior to starting the risk assessment activities or before starting the identification of threats and vulnerabilities, the already implemented security controls should be identified. This is necessary for a complete identification and realistic valuation of the threats and vulnerabilities, and is also important when considering the risk treatment options and what to do to manage the risks (see also Clause **6**). If this identification of already implemented controls has not yet taken place, it is recommended to do it prior to starting the threat/vulnerability assessment.

5.5.2 Identification of threats and vulnerabilities

Assets are subject to many kinds of threats. A threat can cause an unwanted incident which could result in harm to the organization and its assets. This harm can occur from an attack on the organization's information, e.g. resulting in its unauthorized disclosure, modification, corruption, destruction and unavailability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit one or more vulnerabilities of the systems, applications or services used by the organization in order to successfully cause harm to assets. Threats may originate from within the organization as well as external to it. Examples of threats are given in **C.2** and **C.3**.

Vulnerabilities are security weaknesses associated with an organization's assets. These weaknesses could be exploited by one or more threats causing unwanted incidents that might result in loss, damage or harm to these assets and the business of the organization. The vulnerability in itself does not cause harm, it is merely a condition or set of conditions that might allow a threat to exploit it and cause harm to the assets and the business they support. The vulnerability identification should identify the weaknesses related to the assets in the:

- physical environment;
- personnel, management and administration procedures and controls;
- business operations and service delivery;
- hardware, software or communications equipment and facilities.

Examples of vulnerabilities are given in **C.4**.

It should be noted that threats and vulnerabilities need to come together to cause incidents that might damage the assets. It is therefore necessary to understand the relationship between threats and vulnerabilities, i.e. which threat might exploit which of the vulnerabilities.

5.6 Assessment of the threats and vulnerabilities

After identifying the threats and vulnerabilities it is necessary to assess the likelihood that they will come together and cause a risk. This includes assessing the likelihood of threats occurring, and how easily vulnerabilities can be exploited by the threat. More information about the valuation scales that can be used for the assessment of threats and vulnerabilities is contained in **C.5.2**.

The assessment of the likelihood of threats should take account of the following.

- *Deliberate threats.* The likelihood of deliberate threats depends on the motivation, knowledge, capacity and resources available to possible attackers, and the attractiveness of assets to sophisticated attacks.
- *Accidental threats.* The likelihood of accidental threats can be estimated using statistics and experience. The likelihood of these threats might also be related to the organization's proximity to sources of danger, such as major roads or rail routes, and factories dealing with dangerous material such as chemical materials or petroleum. Also the organization's geographical location will affect the possibility of extreme weather conditions. The likelihood of human errors (one of the most common accidental threats) and equipment malfunction should also be estimated.
- *Past incidents.* That is, incidents that have taken place in the past, which illustrate problems in the current protective arrangements.
- *New developments and trends.* This includes reports, news and trends obtained from the Internet, news groups or other organizations that help to assess the threat situation.